

Исследователи безопасности из компании Trend Micro обнаружили крайне разрушительный вариант RaaS-вредоноса под названием Anubis, который продаётся в даркнете как услуга.

Вредонос сочетает шифрование файлов и возможность полного уничтожения данных. После активации этой опции восстановление данных становится невозможным, и эксперты полагают, что это сделано для того, чтобы оказать дополнительное давление на жертву. Своими действиями хакеры подчёркивают возможности программы и давят на жертву в целях быстрого и безоговорочного выкупа.

Изначально Anubis был обнаружен в декабре 2024 года как вариант вредоносной программы Sphinx, основное отличие заключалось в формулировке требования выкупа. Недавно создатели Anubis были замечены в вербовке партнёров на форумах даркнета, предлагая им долю в преступных доходах от 50 до 80% в зависимости от их участия. На данный момент в списке жертв всего восемь человек, но есть предположение, что разработчики могут расширить свою деятельность, когда будут полностью проработаны технические и организационные аспекты.